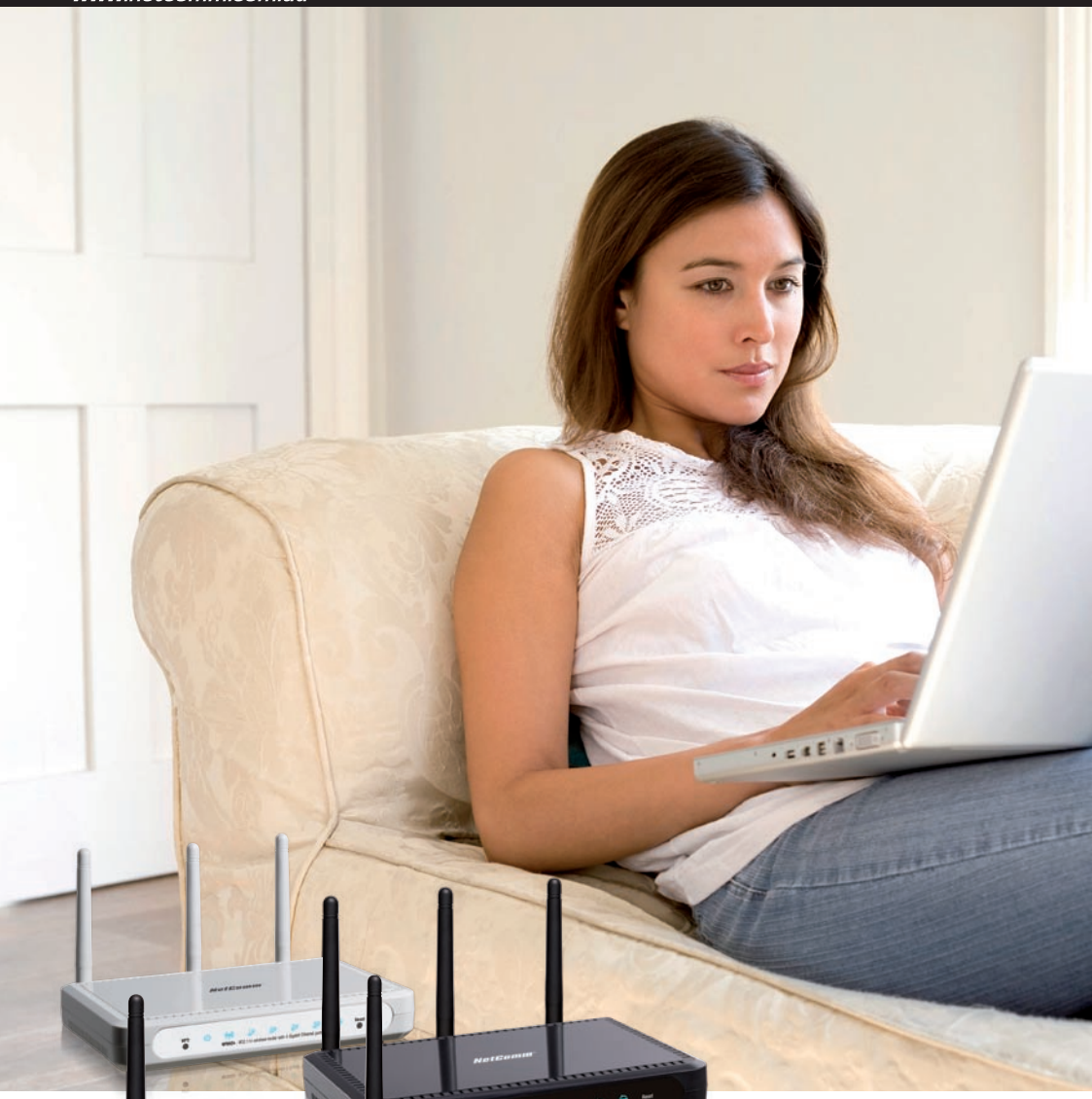
NetComm®
www.netcomm.com.au

Power^{n} Series
802.11 Wireless Router



User Guide

Contents

Introduction 6
Your NetComm Power# Series Router 6
Package Contents 6
Key Features 7

Placement of your Power# Series Router 8
1. Router Placement 8
2. Avoid obstacles and interference 8
3. Cordless Phones 9
4. Choose the "Quitest" Channel for your Wireless Network 9

Product Layout 10

Connecting and Configuring your Router 11
Network and System Requirements 11
Modem Requirements 11
Connecting your Router 12
Configuring your Router 13
PC Network Adapter Setup (Windows XP) 13
Setting up your Router 15

AP Router Mode – Advanced Features 20
Login Procedure 20
System 21
Status 21
LAN 23
DHCP 24
Schedule 25
Event Log 26
Monitor 26
Wizard 27
Internet 28
Status 28
Dynamic IP 28
Static IP 29
Point-to-Point over Ethernet Protocol (PPPoE) 29
Point-to-Point Tunneling Protocol (PPTP) 30

Wireless Settings....31
Basic....31
WDS with AP Router....32
Advanced....33
Security....34
MAC Address Filtering....37
Wi-Fi Protected Setup (WPS)....38
Client List....39
Firewall Settings....40
Demilitarized Zone (DMZ)....41
Denial of Service (DoS)....42
MAC Filter....43
IP Filter....44
URL Filter....45
Advanced Settings....46
Network Address Translation (NAT)....46
Port Mapping....47
Port Forwarding (Virtual Server)....48
Port Triggering (Special Applications)....50
Application Layer Gateway (ALG)....52
UPNP....52
Quality of Service (QoS)....53
Routing....57
Tools Settings....58
Admin....58
Time....59
DDNS....60
Power....61
Diagnosis....61
Firmware....62
Back-up....62
Reset....63

Repeater Mode – Advanced Features 65
System 65
Status 65
LAN 66
Schedule 66
Event Log 67
Monitor 67
Language 67
Wireless Settings 68
Basic 68
Client List 69
Tools Settings 70
Admin 70
Time 71
Power 71
Diagnosis 72
Firmware 72
Back-up 73
Reset ..... 73 got
Legal and Regualtory Information 75

Introduction

Introduction

Your NetComm Power" Series Router

Congratulations on your purchase of NetComm Power" Series Wireless Router. Power" Series is compliant with 802.11n Draft 2.0 up to 6 times faster than standard 802.11g based routers while still being compatible with 802.11g & 802.11b devices. Power" Series is not only a Wireless Access Point, but also doubles as a 4-port full-duplex Ethernet Switch that connects your wired-Ethernet devices together at incredible speeds.

With speeds of up to 300Mbps the NetComm Power" Series Wireless Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple steams of data in a single wireless channel giving you seamless access to multimedia content. Robust RF signal travels farther, eliminates dead spots and extends network range. For data protection and privacy, Power" Series encodes all wireless transmissions with WEP, WPA, and WPA2 encryption.

With inbuilt DHCP Server & powerful SPI firewall Power" Series protects your computers against intruders and most known Internet attacks but provides safe VPN pass-through. With incredible speed and QoS function of 802.11n Draft 2.0, Power" Series is ideal for media-centric applications like streaming video, gaming, and VoIP telephony allowing you to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

Package Contents

1. Power" Series 11n Router
2. 100V~240V Power Adapter
3. RJ45 LAN Cable
4. 2dBi 2.4GHz Dipole Antennas
   - NP800n 2 x Antenna
   - NP801n & NP802n 3 x Antenna
5. Quick Install Guide
6. CD (User's Manual)

Key Features

Features	Advantages
Incredible Data Rate up to 300Mbps**	Heavy data payloads such as MPEG video streaming
IEEE 802.11n Compliant and backward compatible with 802.11b/g	Fully Interoperable with IEEE 802.11b / IEEE 802.11g compliant devices with legacy protection
NP800n & NP801n - Four 10/100 Mbps Fast Switch Ports (Auto-Crossover) NP802n Four Gigabit Fast Switch Ports (Auto-Crossover)	Scalability, extend your network.
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	Avoids the attacks of Hackers or Viruses from Internet
Support 802.1x Authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	Provide mutual authentication (Client and dynamic encryption keys to enhance security
WDS (Wireless Distribution System)	Enables the wireless interconnection of access points in an 802.11 network

** Theoretical wireless signal rate based on IEEE standard of 802.11b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.

Placement of your Power[n] Series Router

Your wireless connection will be stronger the closer your connected device is to your Router. Your wireless connection and performance will degrade as the distance between your Router and connected devices increases. This may or may not be noticeable.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the Router in order to see if distance is the problem. If difficulties persist even at close range, please contact NetComm Technical Support.

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

1. Router Placement

Place your Router, as close as possible to the centre of your wireless network devices. To achieve the best wireless network coverage for your "wireless clients" (i.e., computers enabled by NetComm Wireless USB Adapter, Laptop with Built-in Wireless, Wireless PDA / IPhone):

- Ensure that your Router's antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your Router itself is positioned vertically, point the antennas in an upward direction as much as possible.
- In multi-storey homes, place the Router on a floor that is as close to the centre of the home as possible. This may mean placing the Router on an upper floor.
- Try not to place the Router near a cordless 2.4GHz phone.

2. Avoid Obstacles and Interference

Avoid placing your Router near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path (between your devices and Router).

3. Cordless Phones

If the performance of your wireless network is impaired after attending to the above issues, and you have a cordless phone:

- Try moving cordless phones away from your Router and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Router to channel 11. See your phones user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

4. Choose the "Quietest" Channel for your Wireless Network

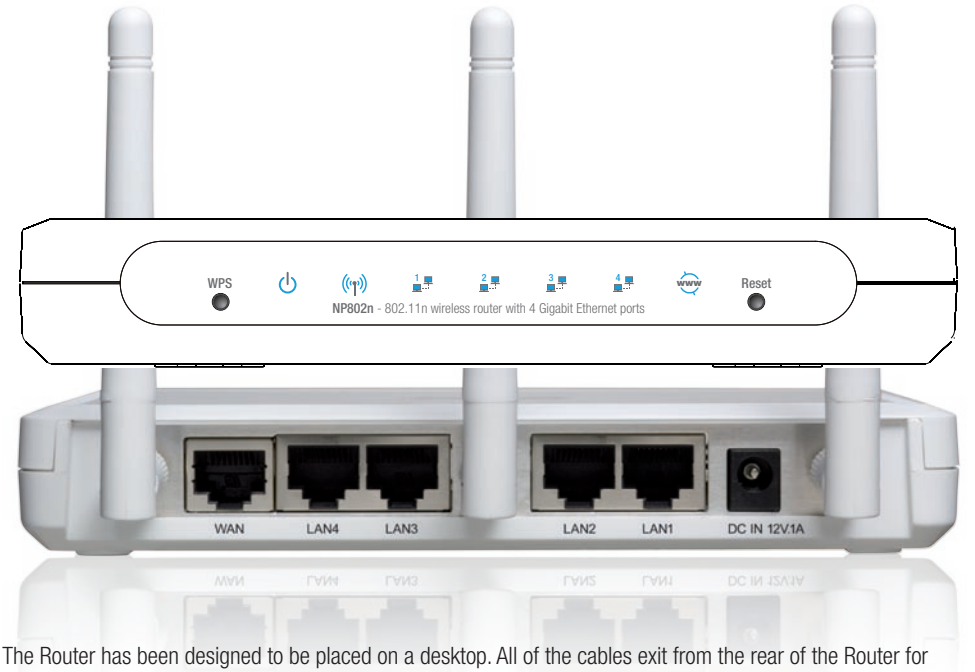
In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with yours.

Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and move your Router and computers to a channel as far away from other networks as possible.

- Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.
- For NetComm wireless networking products, use the detailed Site Survey and wireless channel information included with your wireless network card. See your network card's user guide for more information.

These guidelines should allow you to cover the maximum possible area with your Router. Should you need to cover an even wider area, you should consider looking at building a hybrid network by combining your wireless network with a HomePlug Network. See NetComm website for more details on HomePlug products.

Product Layout



The Router has been designed to be placed on a desktop. All of the cables exit from the rear of the Router for better organization. The display is easily visible on the FRONT of the Router to provide you with information about network activity and status. See below for explanation of each of the features.

Front Panel		
WPS (Wireless Protected Setup)		Click this button to start WPS function.
POWER		Lights up when powered ON. Blinks on TEST/RESET
WLAN (Wireless LAN)		Lights up when WLAN is enabled. Blinks on traffic
LAN PORT ACTIVITY		Blinks on traffic for specific LAN PORT
WAN		Lights up when WAN connection established.
Reset		Click this button to restart the system, or Press this button and hold for 10 seconds to reset to factory defaults.
Rear Ports		
WAN		Wide Area Network(WAN) port
LAN1 ~ 4		Local Area Network (LAN) ports 1 to 4
DC IN		Power connector, connects to DC 12V Power Adapter

Connecting and Configuring your Router

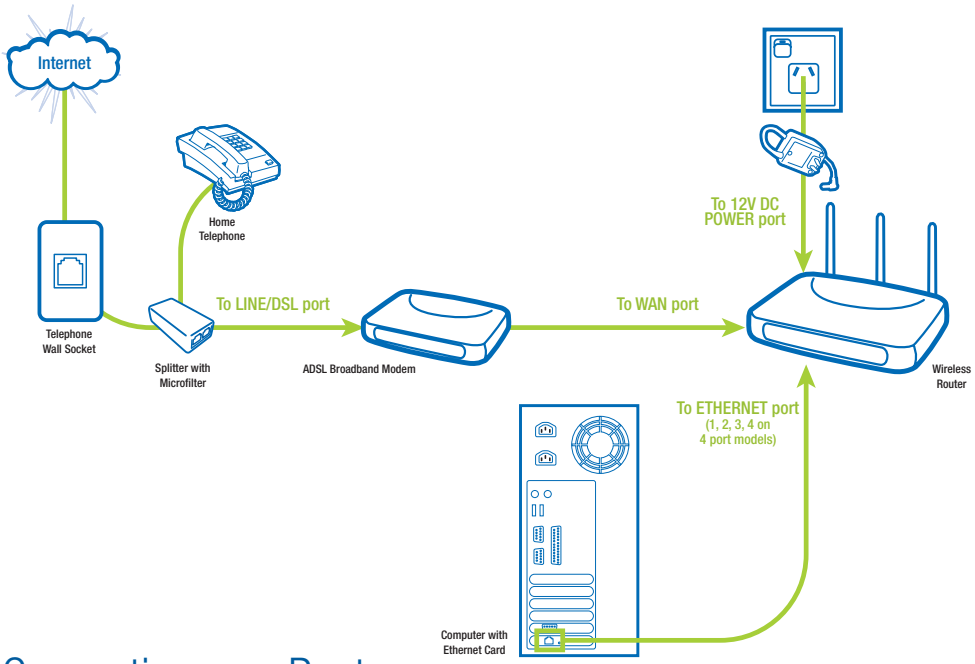
Network + System Requirements

To begin using the 800n Series, make sure you meet the following as minimum requirements:

- PC/Notebook.
- Operating System – Microsoft Windows 98SE/ME/XP/2000/VISTA
- 1 Free Ethernet port on PC/Notebook.
- WiFi card/USB dongle (802.11 a/b/g/n) – optional.
- External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45).
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera etc.)

Modem Requirements

Your cable or DSL modem must be equipped with an RJ45 Ethernet port. Many modems have both an RJ45 Ethernet port and a USB connection. If you have a modem with both Ethernet and USB, and are using the USB connection at this time, you will be instructed to use the RJ45 Ethernet port during the installation procedure. If your modem has only a USB port, you can request a different type of modem from your ISP, or you can purchase a modem that has an RJ45 Ethernet port on it.



Connecting your Router

A Attach your antennas. Place your router next to your modem. Unplug your modem's power cord.

B Locate the networking cable that connects your modem and computer. Unplug that cable from your modem, and plug it into any LAN port on the back of the 900n Series Router.

C Find your new networking cable (included in the box with your 900n series Router) and connect it to the WAN port on the back of the 900n Series Router. Connect the other end to your modem's LAN Port.

D Plug in your modem's power cord. Wait 60 seconds for the modem to start up. Plug the 900n Series Router's power supply into the power socket on the back. Plug the other end into the wall outlet. Turn on the power outlet.

E Wait 20 seconds for the Router to start up. Look at the display on the front of the Router. Make sure the "Power", "LAN" and "WAN" icons are lit up in blue. If they are not, recheck your connections.

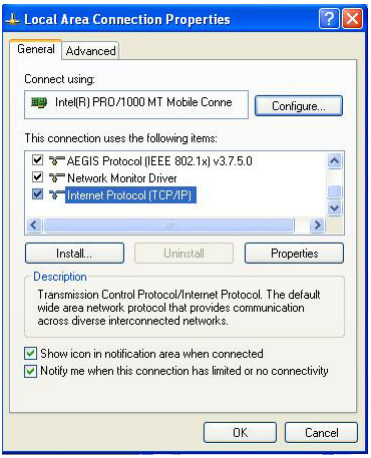
Configuring your Router

PC Network Adapter setup (Windows XP)

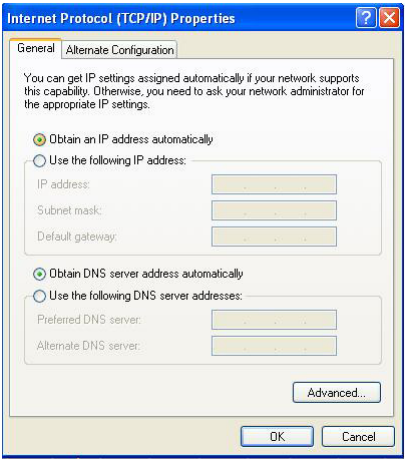
Set your network adapter to obtain an IP Address automaticly (See section on PC Network Adapter setup in this manual for details)

- Click on [Start Menu] > select [Control panel] > select [Network Connections]
- Select [Local Area Connection]) icon > select [properties]

- Select [Internet Protocol (TCP/IP)] > Click [Properties]



- Select the [General] tab
- Please select both
  - Obtain an IP address automatically
  - Obtain DNS server address automatically


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Setting up your Router

- Open a web browser (Internet Explorer, Firefox, etc)
- Type http://192.168.20.1 into the web browser address bar. The below screen will appear.

Connect to 192.168.20.1
The server 192.168.20.1 at Default: admin/admin requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

Type in the default:-

User name **admin**

Password **admin**

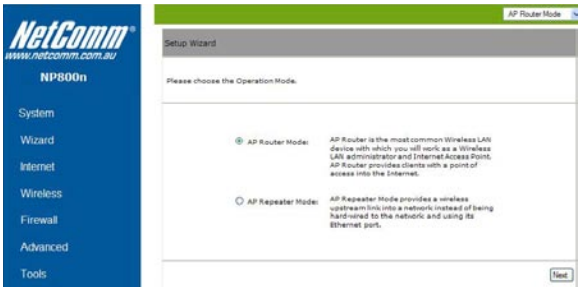
Then Click <OK>.

You are now logged into the router. Select Wizard from the menu on the left hand side

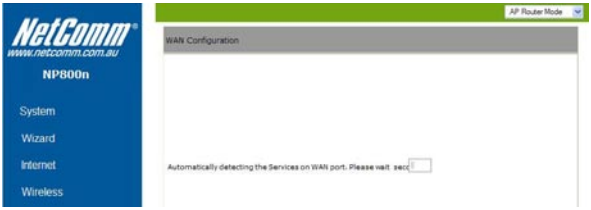
Click <Next> to Start the wizard

The most common of all connections is AP Router Mode. Select this.

For details on AP Repeater Mode see Repeater mode section in this manual.

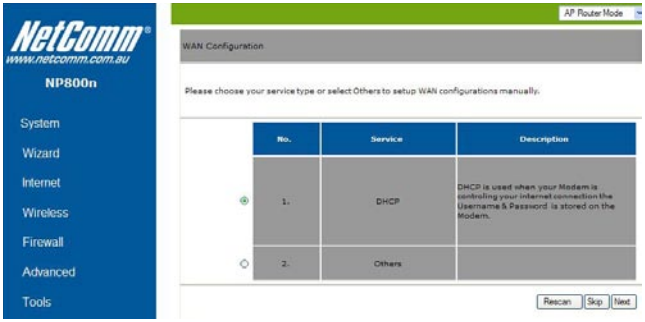

NetComm
www.netcomm.com.au
NP800n
System
Wizard
Internet
Wireless
Firewall
Advanced
Tools
AP Router Mode
Setup Wizard
Please choose the Operation Mode.
AP Router Mode:
AP Router is the most common Wireless LAN device with which you will work as a Wireless LAN administrator and Internet Access Point. AP Router provides clients with a point of access into the Internet.
AP Repeater Mode:
AP Repeater Mode provides a wireless upstream link into a network instead of being hard-wired to the network and using its Ethernet port.
Next

Please wait while your 800n Series router detects your network settings.



For most connections the following options will appear. DHCP is used if you have an existing modem setup with your ISP Username and Password.

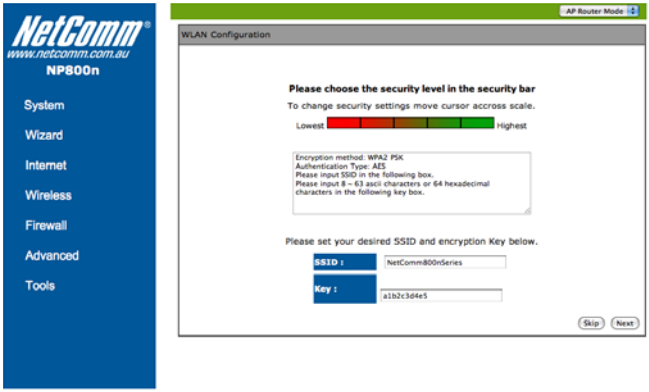
Advanced users Note: If you Bridge your modem you will get a PPPoE option this will then prompt you for ISP Username and Password.



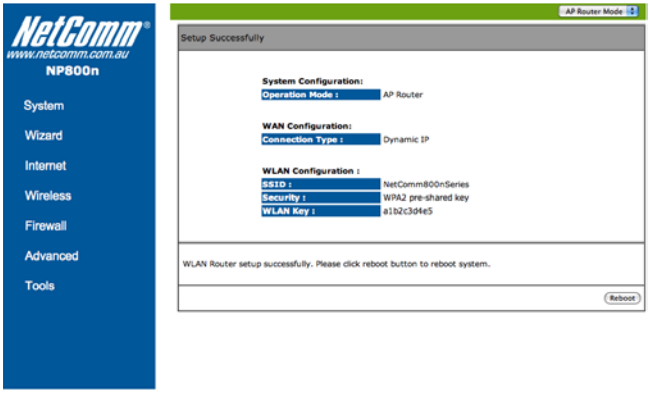
Click <Next> unless you are told by Your ISP to clone your MAC address

To set up your wireless security, hover your mouse over the security bar. The window will tell you what level you have selected. You will then need to set your “SSID”, this is the name of your wireless network. You can use any name. You will then need to select a “Key”.

The Key is your security number (you will need to remember this as you will need to enter this when wirelessly connecting to your network. Click <Next> to proceed.



To apply the entire configuration, click <Reboot>.



AP Router Mode

AP Router Mode – Advanced Features

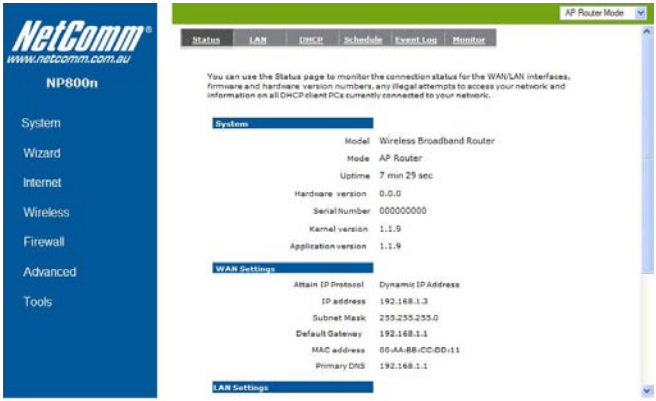
800n Series uses web-interface for configuration to be accessed through your web browser, such as Internet Explorer or Netscape Communicator.

Login Procedure

1. OPEN your browser (e.g. Internet Explorer).
2. Type http://192.168.20.1 in address bar and hit [Enter] button on your keyboard.

Connect to 192.168.20.1
The server 192.168.20.1 at Default: admin/admin requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

3. Click <OK> to navigate into 800n Series configuration home page.
4. You will see the home page of 800n Series as follows.



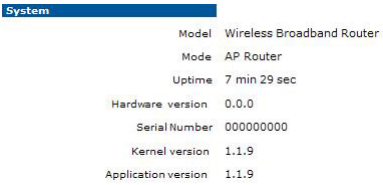
System

Status

This page allows you to monitor the current status of your router. You can use the status page to quickly see if you have any updated firmware available (bug fixes, updates). You can navigate from this page with a few interesting options for reminding or skipping this page forever & so forth.

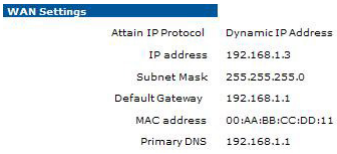
Once you click on <OK> button to go to the requested page, you can see the status page of the 800n Series.

System



You can see the UP time, hardware information, serial number as well as firmware version information.

WAN Settings

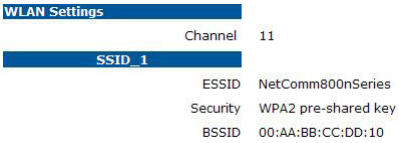


This section displays whether the WAN port is connected to a Cable/DSL connection. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press <Renew> button to renew your WAN IP address.

LAN Settings

This section displays the Broadband router LAN port's current LAN & WLAN information. It also shows whether the DHCP Server function is enabled / disabled.

WLAN Settings

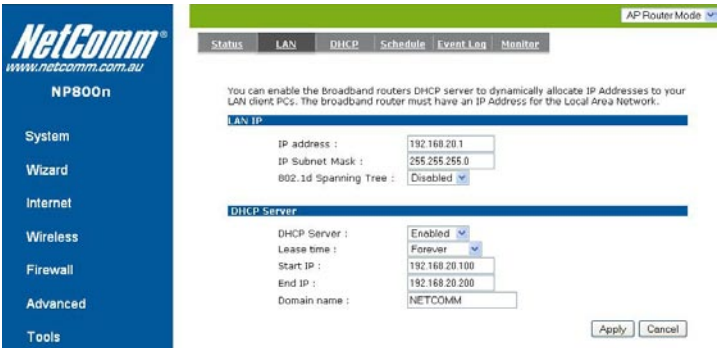


This section displays the current WLAN configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section. Wireless configuration details such as SSID, Security settings, BSSID, Channel number, mode of operation are briefly shown.

LAN

The LAN Tab reveals LAN settings which can be altered. If you are an entry level user, try accessing a website from your browser. If you can access a website without a glitch, just do not change any of these settings.

Click <Apply> at the bottom of this screen to save the changed configurations.



LAN IP

IP address: 192.168.20.1. It is the router's LAN IP address (Your LAN clients default gateway IP address). It can be changed based on your own choice.

IP Subnet Mask: 255.255.255.0 Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree: This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

DHCP Server

DHCP Server: This will enable or disable the Dynamic Pool setting..

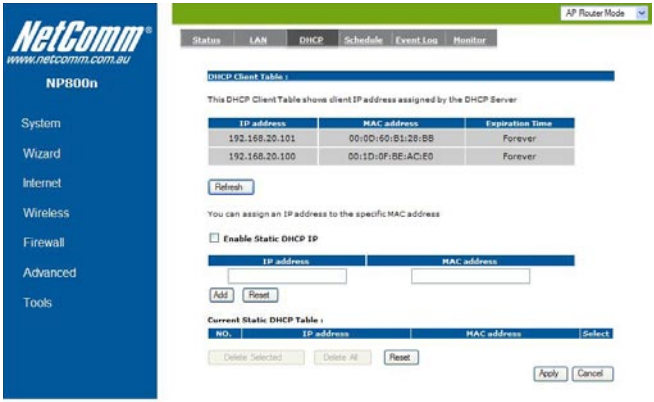
Lease time: This is the lease time of each assigned IP address.

Start IP: This will be the beginning of the pool of IP addresses available for client devices.

End IP: This will be the end of the pool of IP addresses available for client devices.

Domain name: The Domain Name for the existing or customized network.

DHCP

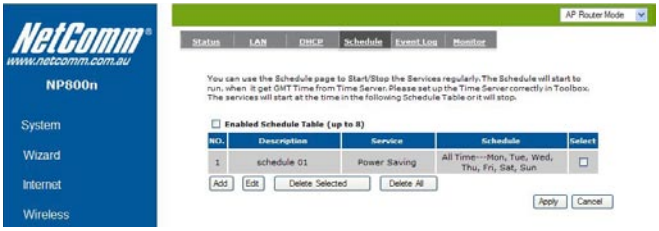


View the current LAN clients which are assigned with an IP Address by the DHCP-server. This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client. Use the <Refresh> button to update the available information. Hit <Refresh> to get the updated table.

You can check “Enable Static DHCP IP“. It is possible to add more static DHCP IPs. They are listed in the table “Current Static DHCP Table“. IP address can be deleted at will from the table.

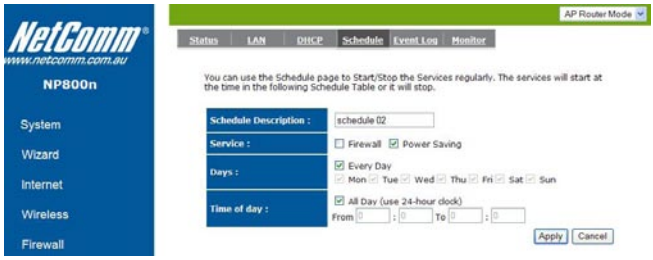
Click <Apply> button to save the changed configuration.

Schedule

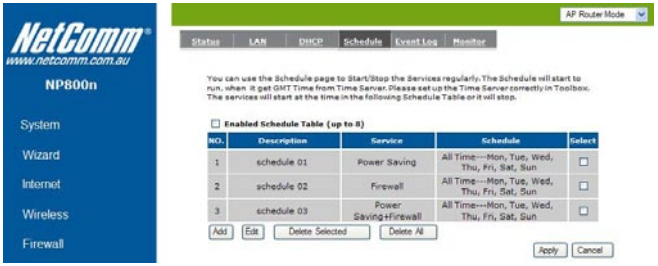


This page allows user to set up schedule function for Firewall and Power Saving.

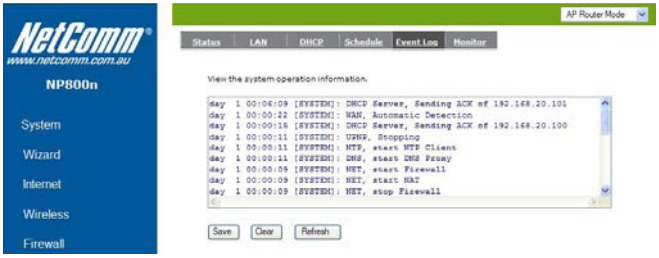
Add schedule, edit schedule options to allow configuration of firewall and power savings services. Fill in the schedule and select type of service. Click <Apply> to implement those settings.



The schedule table lists the pre-schedule service-runs. You can select any of them using the check box.

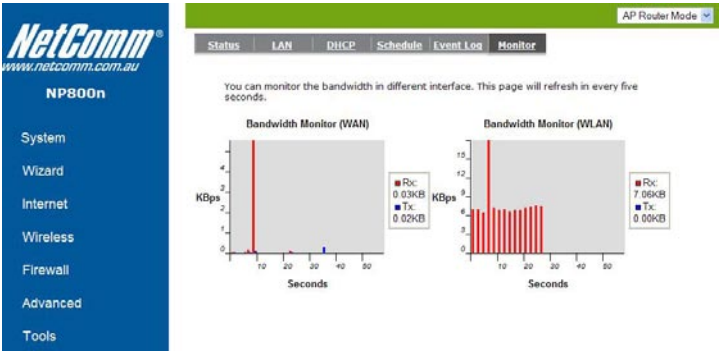


Event Log



View operation event log. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved <Save> to a local file for further processing or the system log can be cleared <Clear> or it can be refreshed <Refresh> to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.

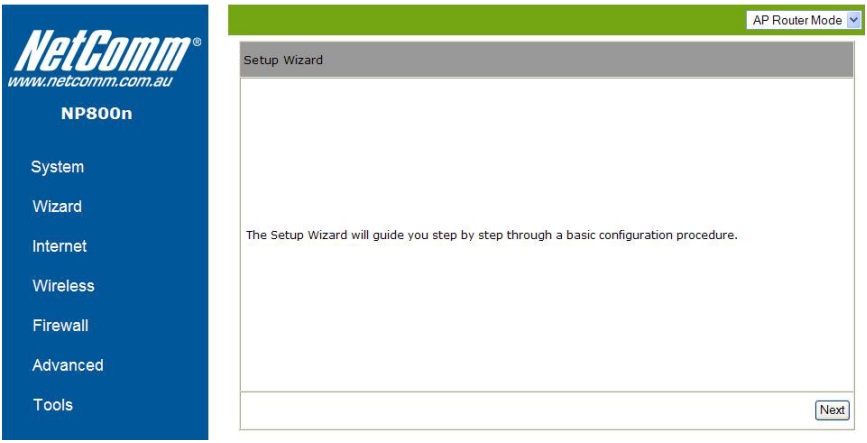
Monitor



Show histogram for network connection on WAN, LAN & WLAN. Auto refresh keeps information updated frequently.

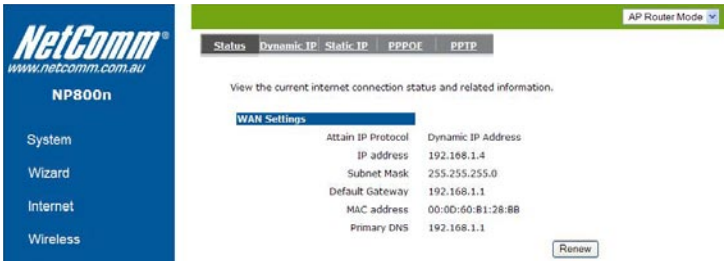
Wizard

Click Wizard to configure the Broadband Router. Setup wizard will now be displayed; check that the modem is connected and click <Next>. For more details please refer to Smart Wizard <Page xx>.



Internet

Status



This page shows the current Internet connection type and status

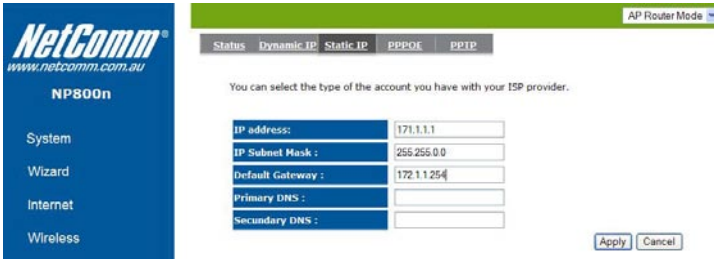
Dynamic IP

Use the MAC address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of the Ethernet card as an identifier, connect only the PC with the registered MAC address to the broadband router and click the <Clone MAC Address> button. This will replace the current MAC address with the already registered Ethernet card MAC address

Host Name: This is optional.

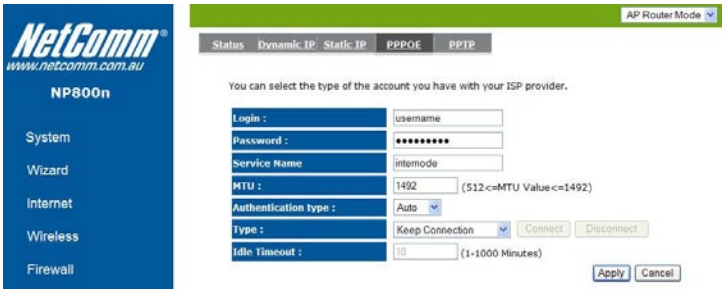
MAC address: The default value is set to the WAN's physical interface of the broadband router.

Static IP



If your ISP Provider has assigned a fixed IP address, enter the assigned IP address, Subnet mask, Default Gateway IP address, and Primary DNS of your ISP provider.

Point-to-Point over Ethernet Protocol (PPPoE)



Login / Password: Enter the PPPoE username and password assigned by your ISP Provider.

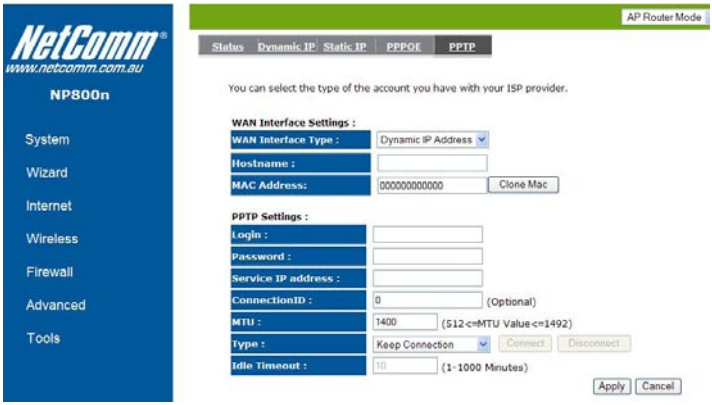
Service Name: This is normally optional.

Maximum Transmission Unit (MTU): This is the maximum size of the packets.

Type: Enable the Auto-reconnect option to automatically re-establish the connection when an application attempts to access the Internet again.

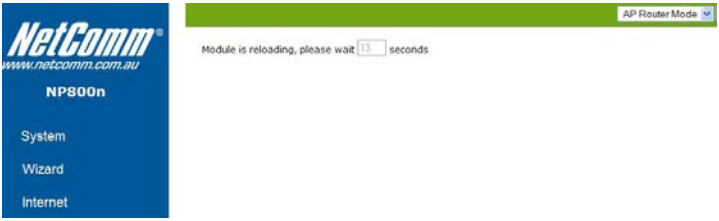
Idle Timeout: This is a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped.

Point-to-Point Tunneling Protocol (PPTP)



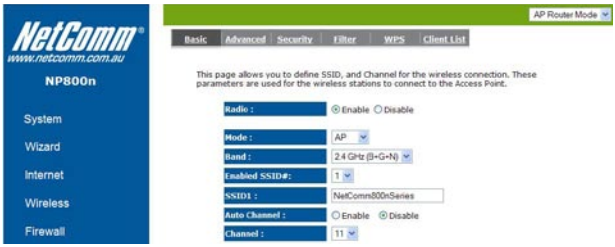
PPTP allows the secure connection over the Internet by simply dialing in a local point provided by your ISP provider. The following screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

Click <Apply> to save configuration and connect to ISP provider.



Wireless Settings

Basic



In basic setting page, you can set wireless Radio, Mode, Band, SSID, and Channel.

Radio: You can turn on/off wireless radio. If wireless Radio is off, you cannot associate with AP through wireless.

Mode: In this device, we support three operation modes which are AP router, AP route with WDS (Page XX), and repeater. If you choose AP Router Mode, you can select AP or WDS function in the drop-down menu.

Band: You can select the wireless standards running on your network environment.

- 2.4 GHz(B): If all your clients are 802.11b, select this one.
- 2.4 GHz(N): If all your clients are 802.11n, select this one.
- 2.4 GHz(B+G): Either an 802.11b or an 802.11g wireless devices are in your environment.
- 2.4 GHz(G): If all your clients are 802.11g, select this one.
- 2.4 GHz(B+G+N): Either 802.11b, 802.11g, or 802.11n wireless devices are in your environment.

Enable SSID: This device supports up to 4 SSIDs. Select the number you would like to use in your network.

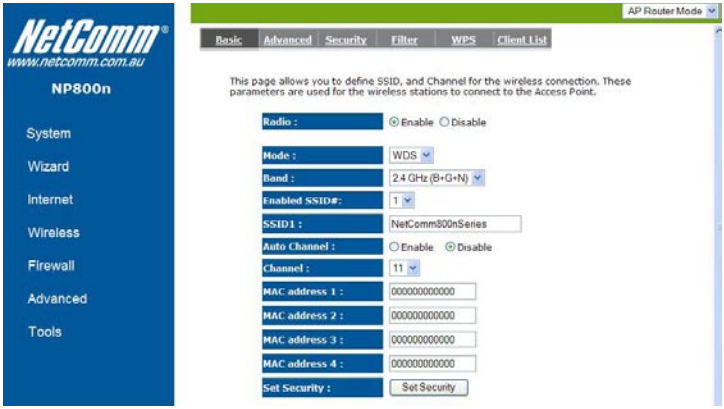
SSID1~4: SSID is the name of your wireless network. Use a unique name to identify this wireless device in the Wireless LAN. It is case sensitive and up to 32 characters. You should change the default SSID for added security.

Auto Channel: Device will search all valid channels, then decide a most clean channel and change to this channel if you enable this function. Depend on this function enable or not, you will see different item below Auto Channel.

Channel: If Auto Channel is disabled, choose a static channel, AP will use this to communicate with other clients.

Check Channel Time: If Auto Channel is enabled, you can choose a period from the drop-down menu. AP will change to a clean channel periodically.

WDS with AP Router



Wireless Distribution System, a system that enables the wireless interconnection of access point, allows a wireless network to be expanded using multiple access points without a wired backbone to link them. Each WDS AP need to be set as same channel and encryption type.

MAC address 1~4: Please enter the MAC address of the neighboring APs that participates in WDS, we support 4 devices now.

Set Security: WDS Security depends on your AP security settings. Note: it does not support mixed mode such as WPA-PSK/WPA2-PSK Mixed mode.

Advanced

NetComm
www.netcomm.com.au
NP800n
System
Wizard
Internet
Wireless
Firewall
Advanced
Tools
AP Router Mode
Basic
Advanced
Security
Filter
WPS
Client List
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.
Fragment Threshold : 2346 (256-2346)
RTS Threshold : 2347 (0-2347)
Beacon Interval : 100 (20-1024 ms)
DTIM Period : 1 (1-10)
Data rate : Auto
N Data rate: Auto
Channel Bandwidth : Auto 20/40 MHZ 20 MHZ
Preamble Type : Long Preamble Short Preamble
CTS Protection : Auto Always None
Tx Power : 100 %

This tab allows you to set the advanced wireless options. You should not change these parameters unless you know what effect the changes will have on the router.

Fragment Threshold: This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold: When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval: Interval of time the wireless router broadcasts a beacon, used to synchronize the wireless network.

DTIM Period: Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages

Data Rate: The “Data Rate” is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

N Data Rate: The “Data Rate” is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.

Channel Bandwidth: This is the range of frequencies that will be used.

Preamble Type: The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance.

CTS Protection: It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

TX Power: This can be set to a bare minimum or maximum power.

Security

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.

SSID Selection: This broadband router support multiple SSID, you could select and set up the wanted SSID.

Broadcast SSID: If you enabled "Broadcast SSID", every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast SSID" can provide better security.

WMM: Wi-Fi MultiMedia if enabled supports QoS for experiencing better audio, video and voice in applications.

Encryption: When you choose to disable encryption, your network is unsecured.

Enable 802.1x Authentication

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

WEP Encryption

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.

Authentication Type: There are two authentication types: “Open System” and “Shared Key”. When you select “Open System”, wireless stations can associate with this wireless router without WEP encryption. When you select “Shared Key”, you should also setup a WEP key in the “Encryption” page. After this has been done, make sure the wireless clients that you want to connect to the device are also setup with the same encryption key.

Key Length: You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

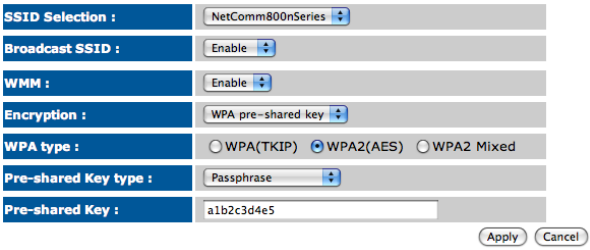
Key Type: You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.

Key1 - Key4: The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys.

128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 13-digit ASCII characters as the encryption keys.

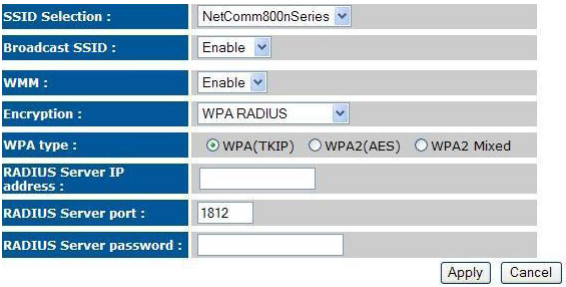
Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-Shared Key Encryption



Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.

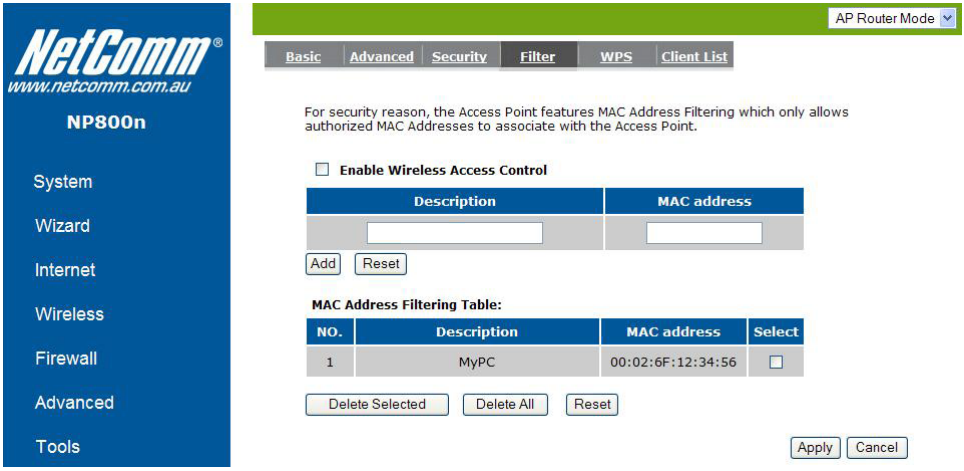
WPA-Radius Encryption



Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication.

It uses TKIP or CCMP (AES) to change the encryption key frequently. Press <Apply> button when you are done.

MAC Address Filtering



This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

Enable wireless access control: Enable the wireless access control function

Adding an address into the list

Enter the "MAC Address" and "Comment" of the wireless station to be added and then click <Add>. The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

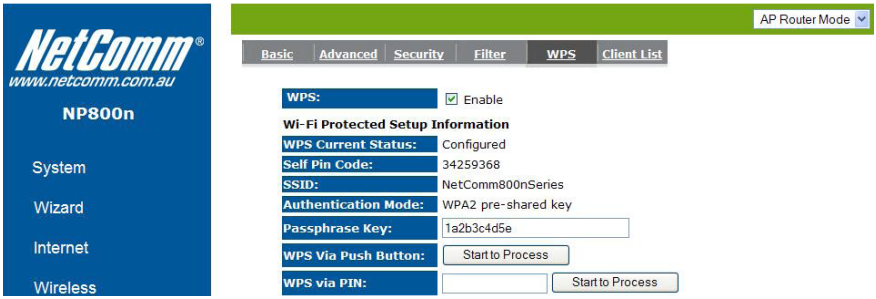
Remove an address from the list

If you want to remove a MAC address from the "Current Access Control List ", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the <Delete All> button. Click <Reset> will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations.

Wi-Fi Protected Setup (WPS)

WPS is the simplest way to establish a connection between wireless clients and the wireless router. You don't have to select the encryption mode and fill in a passphrase. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you. The wireless router supports two types of WPS. **WPS via Push Button** – you have to push a specific button on the wireless client or in your wireless client utility to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. **WPS via PIN code** – you have to know the PIN code of the wireless client and switch it to WPS mode, then input the wireless client PIN to the wireless router web interface.



WPS: Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status: If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.

Self Pin Code: This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID: This is the network broadcast name (SSID) of the router.

Authentication Mode: It shows the active authentication mode for the wireless connection.

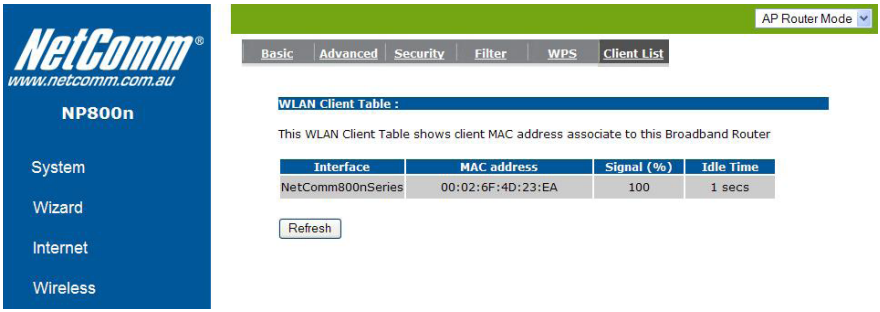
Passphrase Key: It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

Interface: If the device is set to repeater mode, you can choose "Client" interface to connect with other AP by using WPS, otherwise you may choose "AP" interface to do WPS with other clients.

WPS via Push Button: Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN: You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

Client List



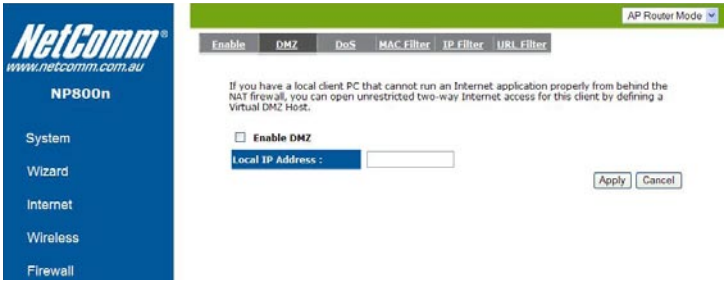
This WLAN Client Table shows the Wireless client associate to this Wireless Router.

Firewall Settings

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select Enable and click Apply

Demilitarized Zone (DMZ)



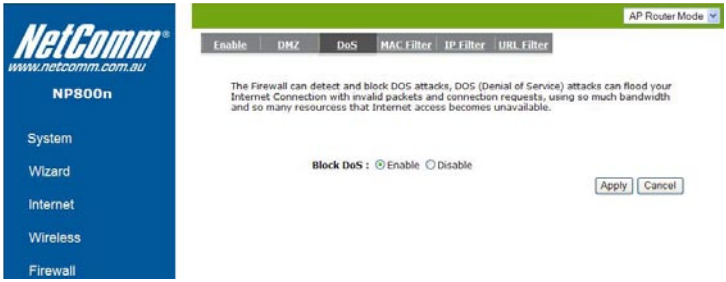
If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

Enable DMZ: Enable/disable DMZ

LAN IP Address: Fill-in the IP address of a particular host in your LAN Network that will receive all the packets originally going to the WAN port/Public IP address above.

Click <Apply> at the bottom of the screen to save the above configurations.

Denial of Service (DoS)



The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

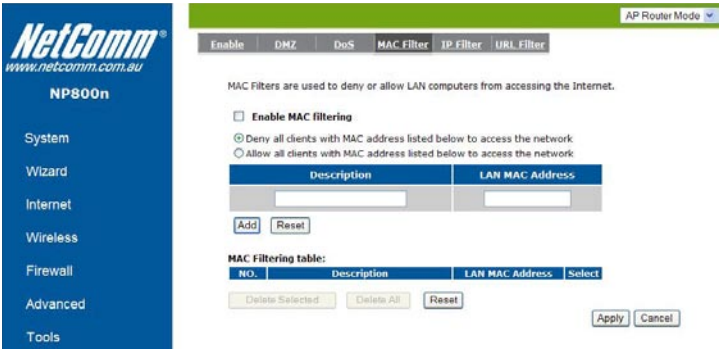
Ping of Death: Protections from Ping of Death attack.

Discard Ping From WAN: The router's WAN port will not respond to any Ping requests

Port Scan: Protects the router from Port Scans.

Sync Flood: Protects the router from Sync Flood attack.

MAC Filter



If you want to restrict users from accessing certain Internet applications / services (e.g. Internet websites, email, FTP etc.), and then this is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Enable MAC Filtering: Check to enable or disable MAC Filtering.

Deny: If you select "Deny" then all clients will be allowed to access Internet except for the clients in the list below.

Allow: If you select "Allow" then all clients will be denied to access Internet except for the PCs in the list below.

Add PC MAC Address

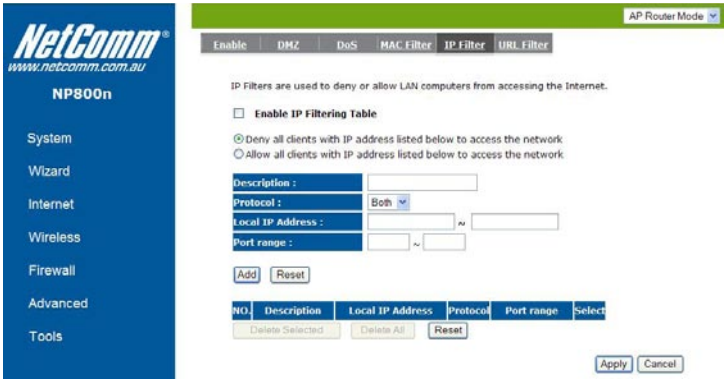
Fill in "LAN MAC Address" and <Description> of the PC that is allowed to access the Internet, and then click <Add>. If you find any typo before adding it and want to retype again, just click <Reset> and the fields will be cleared.

Remove PC MAC Address

If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click <Delete Selected>. If you want to remove all PCs from the table, just click the <Delete All> button. If you want to clear the selection and re-select again, just click <Reset>.

Click <Apply> at the bottom of the screen to save the above configurations.

IP Filter



Enable IP Filtering: Check to enable or disable IP Filtering.

Deny: If you select “Deny” then all clients will be allowed to access Internet except for the clients in the list below.

Allow: If you select “Allow” then all clients will be denied to access Internet except for the PCs in the list below.

Add PC IP Address

You can click <Add> PC to add an access control rule for users by an IP address or IP address range.

Remove PC IP Address

If you want to remove some PC IP from the <IP Filtering Table>, select the PC you want to remove in the table and then click <Delete Selected>. If you want to remove all PCs from the table, just click the <Delete All> button.

Click <Apply> at the bottom of the screen to save the above configurations.

URL Filter

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.

Enable URL Blocking: Enable or disable URL Blocking

Add URL Keyword

Fill in "URL/Keyword" and then click <Add>. You can enter the full URL address or the keyword of the web site you want to block. If you happen to make a mistake and want to retype again, just click "Reset" and the field will be cleared.

Remove URL Keyword

If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click <Delete Selected>.

If you want to remove all URL keywords from the table, click <Delete All> button. If you want to clear the selection and re-select again, just click <Reset>.

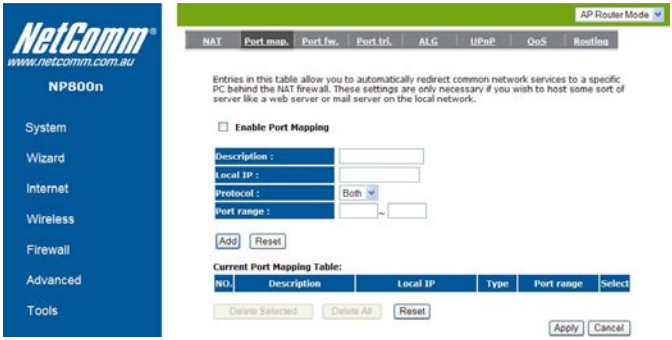
Click <Apply> at the bottom of the screen to save the above configurations

Advanced Settings

Network Address Translation (NAT)

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.

Port Mapping



Port Mapping allows you to re-direct a particular range of service port numbers (from the Internet / WAN Port) to a particular LAN IP address. It helps you to host servers behind the router NAT firewall.

Enable Port Mapping: Enable or disable port mapping function.

Description: description of this setting.

Local IP: This is the local IP of the server behind the NAT firewall.

Type: This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only, or select “BOTH” to forward both “TCP” and “UDP” packets.

Port Range: The range of ports to be forward to the private IP.

Add Port Mapping

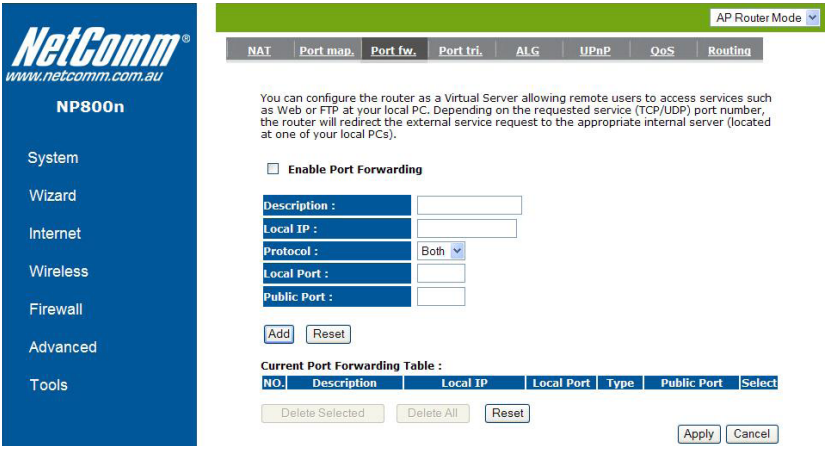
Fill in the “Local IP”, “Type”, “Port Range” and “Description” of the setting to be added and then click “Add”. Then this Port Mapping setting will be added into the “Current Port Mapping Table” below. If you find any typo before adding it and want to retype again, just click <Clear> and the fields will be cleared.

Remove Port Mapping

If you want to remove a Port Mapping setting from the “Current Port Mapping Table”, select the Port Mapping setting that you want to remove in the table and then click D<Delete Selected>. If you want to remove all Port Mapping settings from the table, click <Delete All> button. Click <Reset> will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations.

Port Forwarding (Virtual Server)



Use the Port Forwarding (Virtual Server) function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number. (See Glossary for an explanation on Port number).

Enable Port Forwarding: Enable or disable Port Forwarding.

Description: The description of this setting.

Local IP/Local Port: The LAN Client/Host IP address and Port number the Public Port number packet will be sent to.

Type: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "both" setting. Public Port enters the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN Network.

Public Port: Port number will be changed to Local Port when the packet enters your LAN Network.

Add Port Forwarding

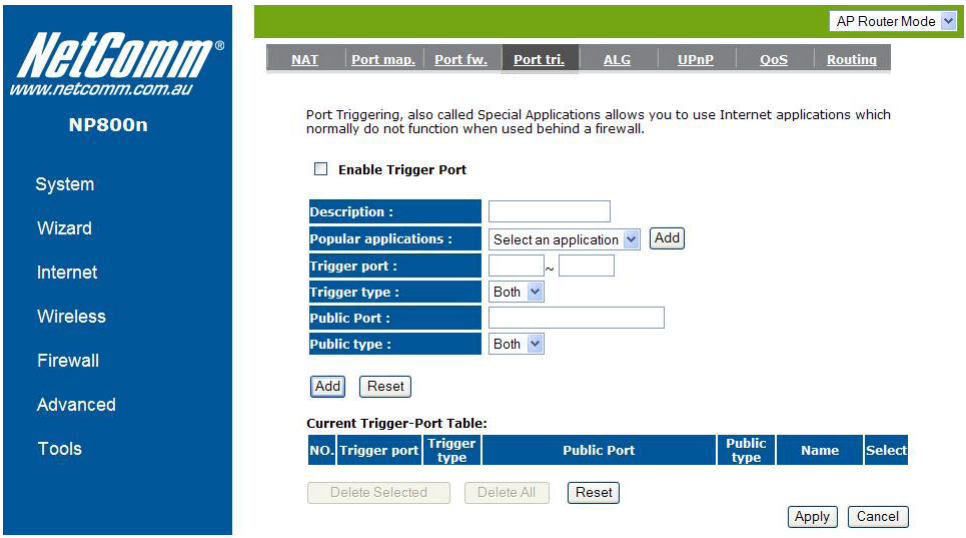
Fill in the “Description” , “Local IP”, “Local Port”, “Type” and “Public Port” of the setting to be added and then click <Add> button. Then this Virtual Server setting will be added into the “Current Port Forwarding Table” below. If you find any typo before adding it and want to retype again, just click <Clear> and the fields will be cleared.

Remove Port Forwarding

If you want to remove Port Forwarding settings from the “Current Port Forwarding Table”, select the Port Forwarding settings you want to remove in the table and then click “Delete Selected”. If you want to remove all Port Forwarding settings from the table, just click the <Delete All> button. Click <Reset> will clear your current selections.

Click <Apply> at the bottom of the screen to save the above configurations.

Port Triggering (Special Applications)



Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

Enable Trigger Port: Enable or disable the Port Trigger function.

Trigger Port: This is the outgoing (Outbound) range of port numbers for this particular application.

Trigger Type: Select whether the outbound port protocol is “TCP”, “UDP” or “BOTH”.

Public Port: Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624)

Public Type: Select the Inbound port protocol type: “TCP”, “UDP” or “BOTH”

Popular Applications: This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

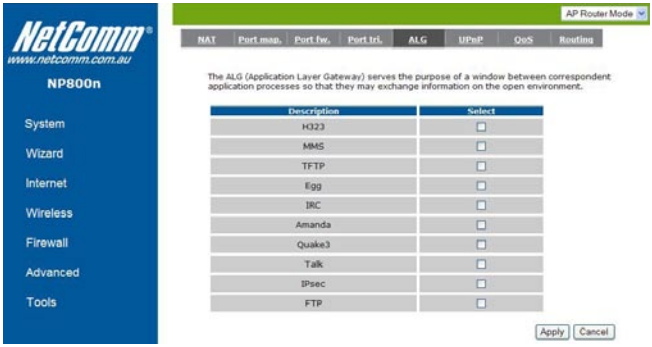
Add Port Triggering

Fill in the “Trigger Port”, “Trigger Type”, “Public Port”, “Public Type”, “Public Port” and “Description” of the setting to be added and then Click <Add>. The Port Triggering setting will be added into the “Current Trigger-Port Table” below. If you happen to make a mistake, just click <Clear> and the fields will be cleared.

Remove Port Triggering

If you want to remove Special Application settings from the “Current Trigger-Port Table”, select the Port Triggering settings you want to remove in the table and then click <Delete Selected>. If you want remove all Port Triggering settings from the table, just click the <Delete All> button. Click <Reset> will clear your current selections.

Application Layer Gateway (ALG)



You can select applications that need ALG support. The router will let the selected application to correctly pass through the NAT gateway.

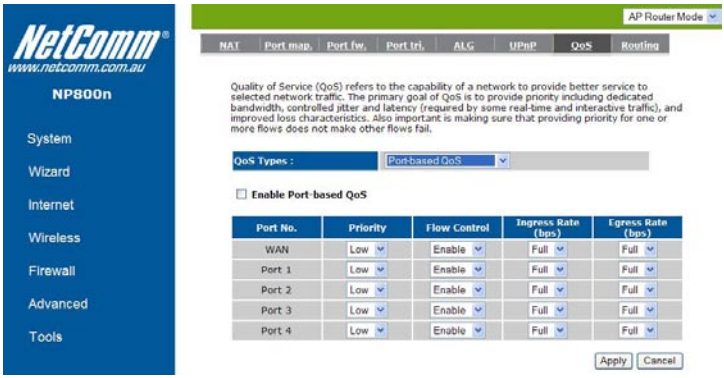
UPNP

With UPnP, all PCs in you Intranet will discover this router automatically. So, you don't have to configure your PC and it can easily access the Internet through this router.

Enable/Disable UPnP: You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

Quality of Service (QoS)

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference … etc. All the applications not specified by you are classified as rule "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.



Port-based QoS

This is hardware port-based QoS control method. It will limit the packets throughput in LAN1~4, WAN port.

Enable Port-based QoS: Check this to enable port-based QoS functionality for the LAN/WAN port. You can also uncheck to disable.

Priority: High or Low priority level of the transmit packets.

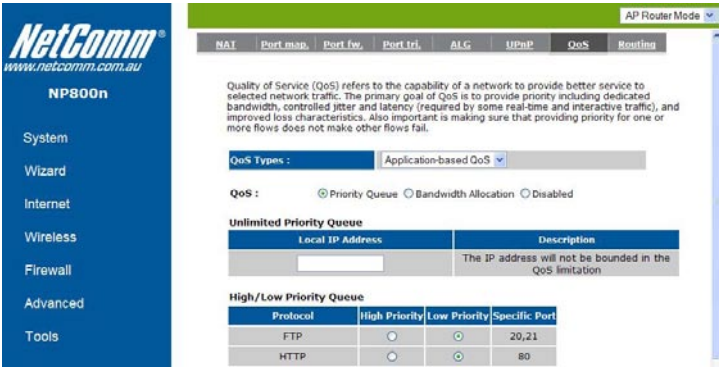
Ingress Rate: The throughput limit of receiving packets.

Egress Rate: The throughput limit of sending packets.

Application-based QoS

This is the application based QoS control method. You can reserve or limit the bandwidth of some LAN IP address and port number. They will guarantee the throughput in WAN connection.

Priority Queue Type:

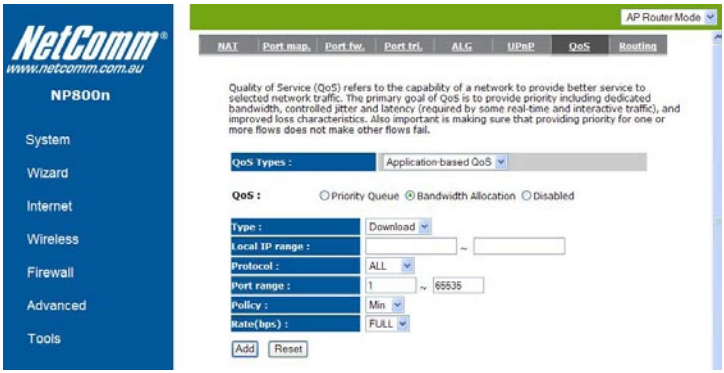


This can put the packets of specific protocols in High/Low Queue. The packets in High Queue will process first.

Unlimited Priority Queue: The LAN IP address will not be bounded in the QoS limitation.

High/Low Priority Queue: This can put the packets in the protocol and port range to High/Low QoS Queue.

Bandwidth Allocation:



This can reserve/limit the throughput of specific protocols and port range. You can set the upper bound and Lower bound.

Type: Specify the direction of packets. Upload or download.

IP range: Specify the IP address range. You could also fill one IP address

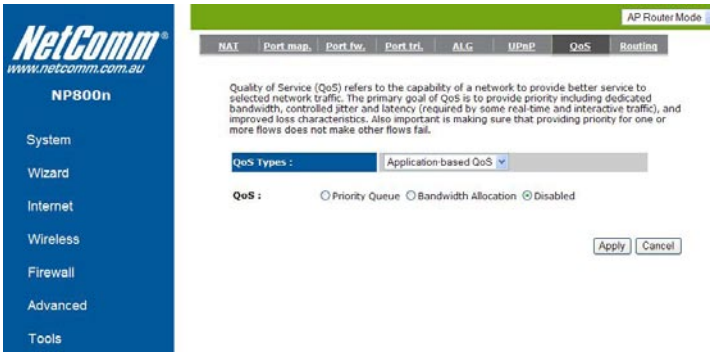
Protocol: Specify the packet type. The default ALL will put all packets in the QoS priority Queue.

Port range: Specify the Port range. You could also fill one Port.

Policy: Specify the policy the QoS, Min option will reserve the selected data rate in QoS queue. Max option will limit the selected data rate in QoS queue.

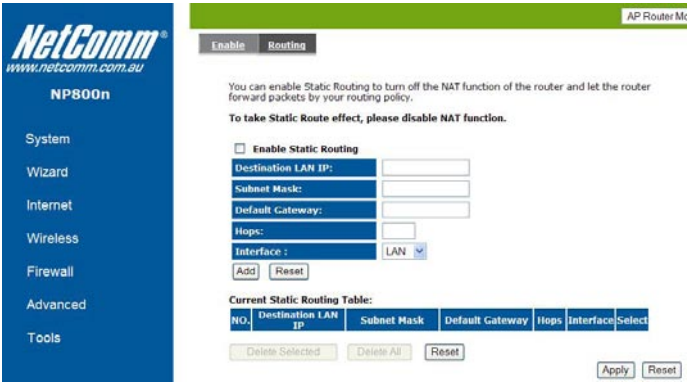
Rate: The data rate of QoS queue.

Disabled



This could turn off QoS feature.

Routing



You can set enable Static Routing to let the router forward packets by your routing policy.

Destination LAN IP: Specify the destination LAN IP address of static routing rule.

Subnet Mask: Specify the Subnet Mask of static routing rule.

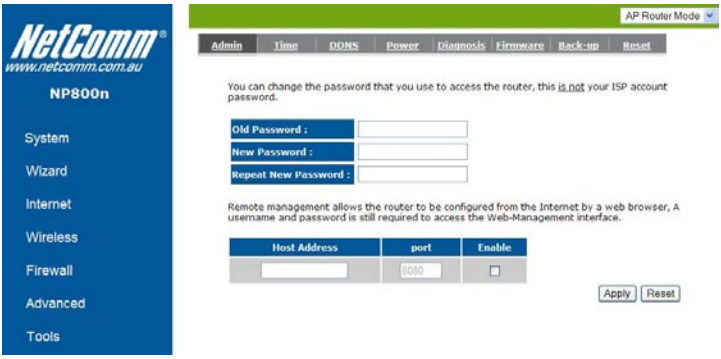
Default Gateway: Specify the default gateway of static routing rule.

Hops: Specify the Max Hops number of static routing rule.

Interface: Specify the Interface of static routing rule.

Tools Settings

Admin



You can change the password required to log into the broadband router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

Current Password: Fill in the current password to allow changing to a new password.

New Password: Enter your new password and type it again in Repeat New Password for verification purposes

Remote management

This allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

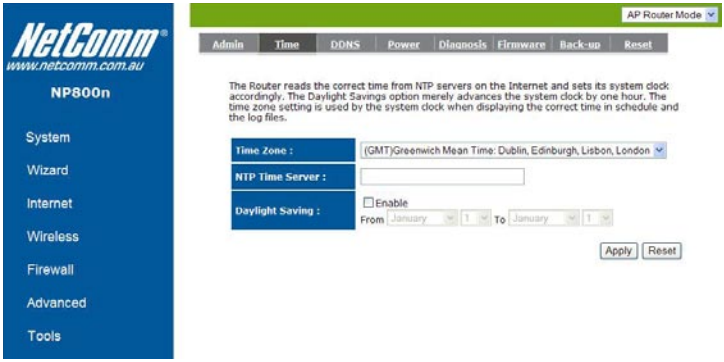
Host Address: This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

Port: The port number of the remote management web interface.

Enabled: Check to enable the remote management function.

Click <Apply> at the bottom of the screen to save the above configurations.

Time



The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

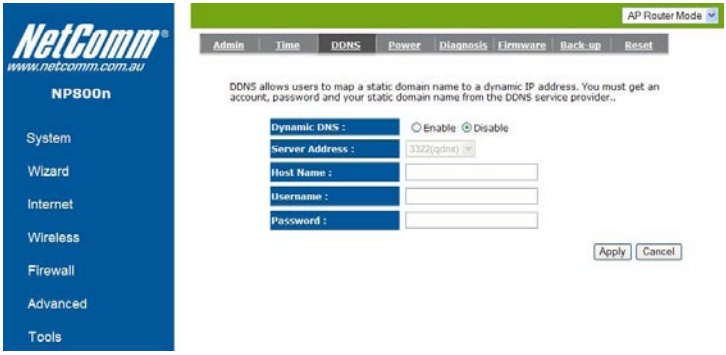
Time Zone: Select the time zone of the country you are currently in. The router will set its time based on your selection.

NTP Time Server: The router can set up external NTP Time Server.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click <Apply> at the bottom of the screen to save the above configurations.

DDNS



DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

Enable/Disable DDNS: Enable or disable the DDNS function of this router

Server Address: Select a DDNS service provider

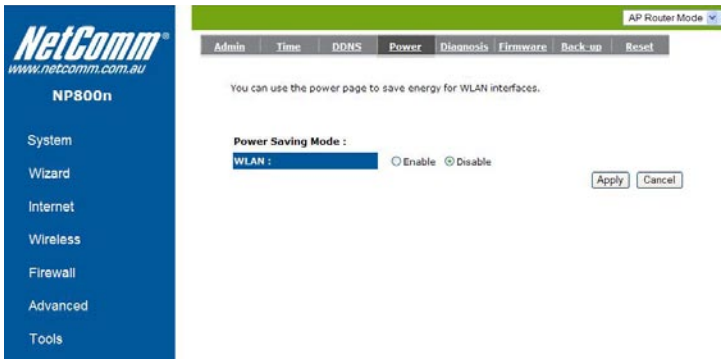
Host Name: Fill in your static domain name that uses DDNS.

Username: The account that your DDNS service provider assigned to you.

Password: The password you set for the DDNS service account above

Click <Apply> at the bottom of the screen to save the above configurations.

Power

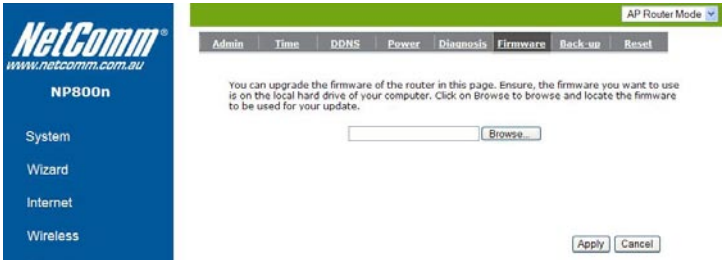


Saving power in WLAN/Ethernet mode can be enabled/disabled in this page.

Diagnosis

This page could let you diagnosis your current network status.

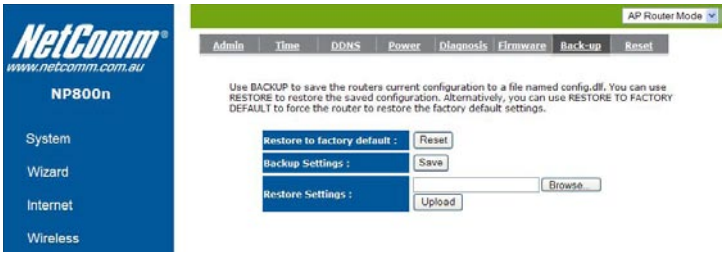
Firmware



This page allows you to upgrade the router's firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <Apply> at the bottom of the screen to start the upgrade process

Back-up



This page allows you to save the current router configurations. When you save the configurations, you also can re-load the saved configurations into the router through the Restore Settings. If extreme problems occur you can use the Restore to Factory Defaults to set all configurations to its original default settings.

Backup Settings: This can save the Broadband router current configuration to a file named "config.bin" on your PC. You can also use the <Upload> button to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

Reset

You can reset the broadband router when system stops responding correctly or stop functions.

Repeater Mode

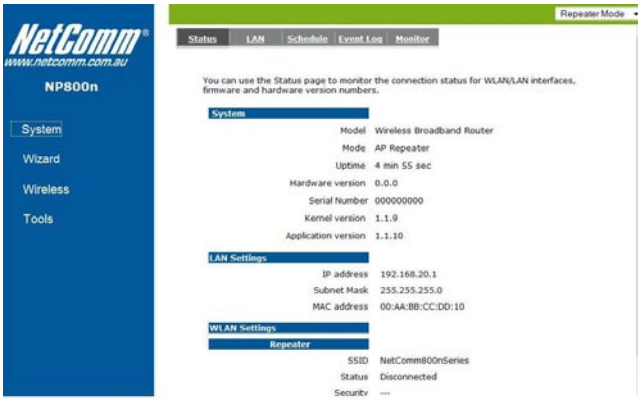
Repeater Mode – Advanced Features

Repeater mode has limited settings compared to the AP mode. Choose “Repeater mode” on the top right corner of the configuration page. System restarts and connects to the IP address http://192.168.20.1

You will see the configuration homepage under “REPEATER” mode now.

System

Status



System status section allows you to monitor the current status of your router. You can use the status page to quickly see if you have any updated firmware available (bug fixes, updates). You can navigate from this page with a few interesting options for reminding or skipping this page forever & so forth.

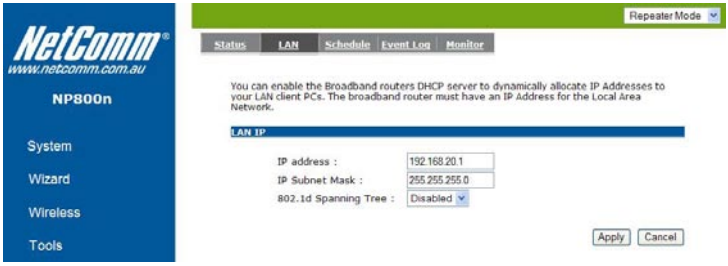
Once you click on <OK> button to go to the requested page, you can see the status page of the 800n Series.

You can see the UP time, hardware information, serial number as well as firmware version information.

LAN Settings: This page displays the Broadband router LAN port’s current LAN & WLAN information. It also shows whether the DHCP Server function is enabled / disabled. Wireless configuration details such as SSID, Security settings, BSSID, Channel number, mode of operation are briefly shown.

WLAN Settings: View Broadband router’s current configuration settings. Device Status displays the configuration settings you’ve configured in the Wizard / Basic Settings / Wireless Settings section

LAN



The LAN Tabs reveals LAN settings which can be altered at will. If you are an entry level user, try accessing a website from your browser. If you can access website without a glitch, just do not change any of these settings.

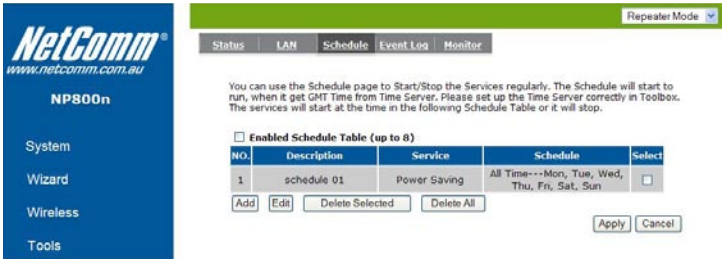
Click <Apply> at the bottom of this screen to save the changed configurations.

IP address: It is the router's LAN IP address (Your LAN clients default gateway IP address). It can be changed based on your own choice.

IP Subnet Mask: Specify a Subnet Mask for your LAN segment.

802.1d Spanning Tree: This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

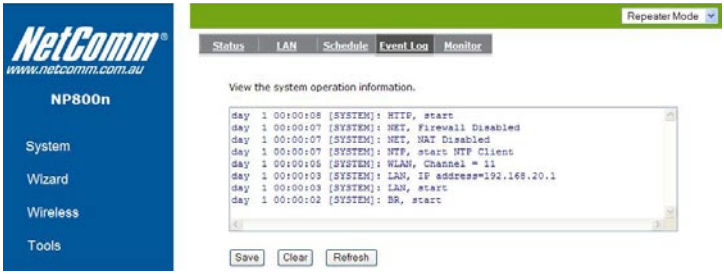
Schedule



Add schedule, edit schedule options allow configuration of power savings services. Fill in the schedule and select type of service. Click <Apply> to implement the settings.

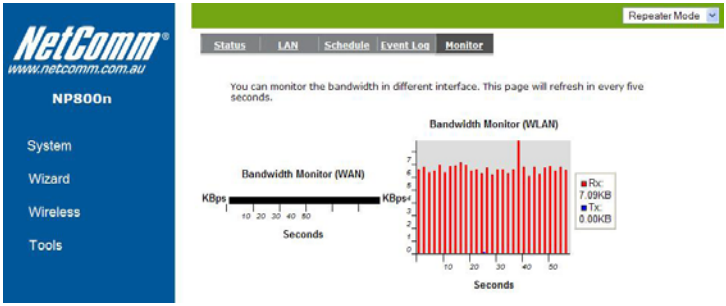
The schedule table lists the pre-schedule service-runs. You can select any of them using the check box.

Event Log



View operation log of 800n Series. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved <Save> to a local file for further processing or the system log can be cleared <Clear> or it can be refreshed <Refresh> to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.

Monitor



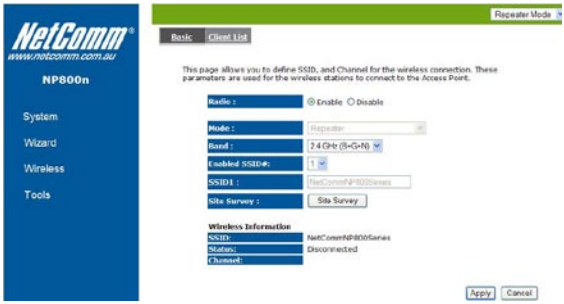
Show the network packets histogram for network connection on WAN, LAN & WLAN. Auto refresh keeps information updated frequently.

Language

This Wireless Router support multiple language of web pages, you could select your native language here.

Wireless

Basic



You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, SSID, Channel Number and Associated Client.

Radio: Enable or Disable Wireless function

Mode:

Band: Allows you to set the AP fixed at 802.11b, 802.11g or 802.11n mode. You can also select B+G mode to allow 802.11b and 802.11g clients at the same time.

Enable SSID: You can specify the maximum SSID number.

SSID1~3: Allow you to specify SSID of WLAN.

Site Survey: You can scan the current Wireless Access Point and connect on it.

Site Survey
NO. Select Channel SSID BSSID Encryption Auth Signal (%) Mode
1 1 11gb 00:03:79:11:74:90 TKIP WPAPSK 100 11b/g
2 1 default 00:03:79:11:72:D0 NONE OPEN 100 11b/g
3 3 NetCommOfficeHotspot 00:60:64:14:49:B0 NONE OPEN 50 11b/g
4 6 NtcOffice 00:60:64:19:C6:40 WEP OPEN 55 11b/g
5 6 test NB11W 00:1A:2B:6D:F5:B9 NONE OPEN 99 11b/g
6 11 Netcomm 7 Series 00:60:64:23:2E:6B WEP OPEN 100 11b/g
7 11 NetCommNP800Series 00:02:6F:51:F9:14 NONE OPEN 100 11b/g/n
8 11 kenken 00:02:6F:50:77:0C AES WPA2PSK 100 11b/g/n
Refresh
Connect

Client List

NetComm
www.netcomm.com.au
NP800n
System
Wizard
Wireless
Tools
Repeater Mode
Basic
Client List
WLAN Client Table :
This WLAN Client Table shows client MAC address associate to this Broadband Router
Interface
MAC address
Signal (%)
Idle Time
No client connecting to the Router.
Refresh

Tools

This section has many useful and miscellaneous features.

Admin

You can change the password required to log into the broadband router's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

Current Password: Fill in the current password to allow changing to a new password.

New Password: Enter your new password and in Repeat New Password for verification purposes

Click <Apply> at the bottom of the screen to save the above configurations

Remote management

This allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address: This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

Port: The port number of the remote management web interface.

Enabled: Check to enable the remote management function.

Click <Apply> at the bottom of the screen to save the above configurations.

Time

The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Event Log entries and Schedule settings.

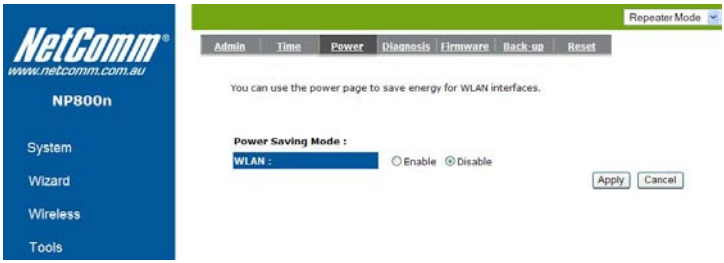
Time Zone: Select the time zone of the country you are currently in. The router will set its time based on your selection.

NTP Time Server: This accept local the IP Address of Local NTP Time Server Address.

Daylight Savings: The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click <Apply> at the bottom of the screen to save the above configurations

Power



Saving power in WLAN/Ethernet mode can be enabled / disabled in this page.

Diagnosis

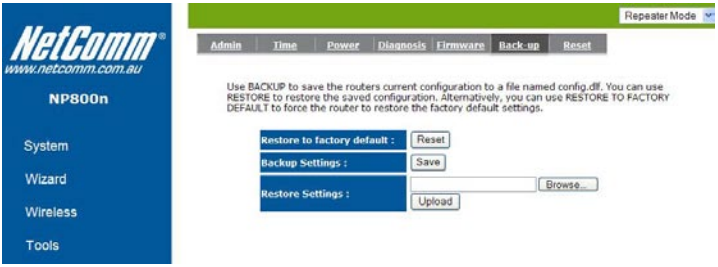
This page could let you diagnosis your current network status.

Firmware

This page allows you to upgrade the router's firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <Apply> at the bottom of the screen to start the upgrade process

Back-up



The page allows you to save (Backup) the router's current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).

Restore Settings: This can save the Broadband router current configuration to a file named "config.bin" on your PC. You can also use the <Upload> button to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" to force the Broadband router to perform a power reset and restore the original factory settings.

Reset

You can reset the broadband router when system stops responding correctly or stop functions.

Legal & Regulatory

Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at

www.netcomm.com.au

NetComm®
www.netcomm.com.au

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website **www.netcomm.com.au**.

Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

www.netcomm.com.au/support

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.

NetComm®
www.netcomm.com.au

NETCOMM LIMITED PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au

Dynalink
www.dynalink.co.nz

DYNALINK NZ 224b Bush Road, Albany, Auckland, New Zealand
P: 09 448 5548 **F:** 09 448 5549
E: sales@dynalink.co.nz **W:** www.dynalink.co.nz

Trademarks and registered trademarks are the property of NetComm Limited or their respective owners.
Specifications are subject to change without notice. Images shown may vary slightly from the actual product.